Bloque IV: El nivel de red

Tema 12: ICMP

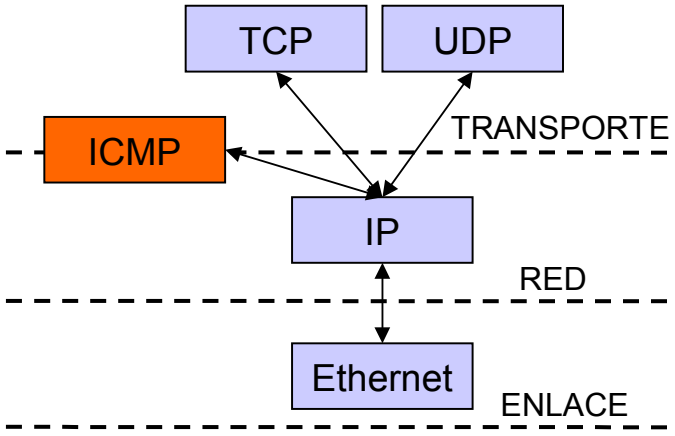
Índice

- Bloque IV: El nivel de red
  - Tema 12: ICMP
    - Introducción
    - Ping
    - Mensajes ICMP de error
    - Traceroute

- **Lecturas recomendadas:**
  - Capítulo 4, sección 4.4.3, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.
  - Capítulo 8 de “TCP/IP Illustrated, Volume 1: The Protocols”, W. Richard Stevens, Addison Wesley.

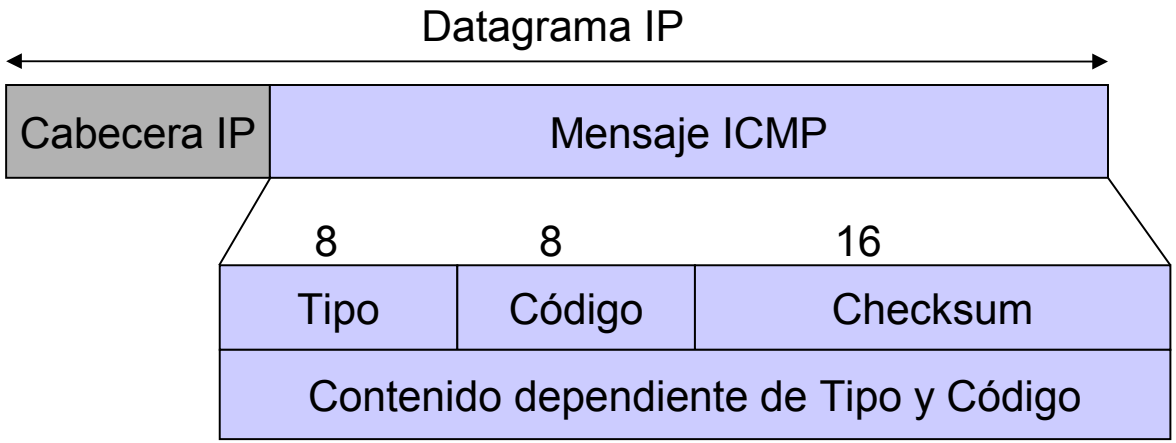
Introducción

- Internet Control Message Protocol
- IP no tiene mecanismos para obtener información de diagnóstico → Para eso está ICMP.
- ICMP comunica mensajes de error y otras condiciones que requieren atención.
- Los mensajes ICMP se transmiten dentro de datagramas IP (RFC 792)
- Dos tipos de mensajes: error y consulta.
- Mensajes ICMP más empleados:
  - Petición y respuesta de eco → ping
  - Destino inalcanzable
    - Puerto inalcanzable
    - Máquina o red inalcanzable
  - Redirect
  - Fragmentación requerida
  - Time excedido



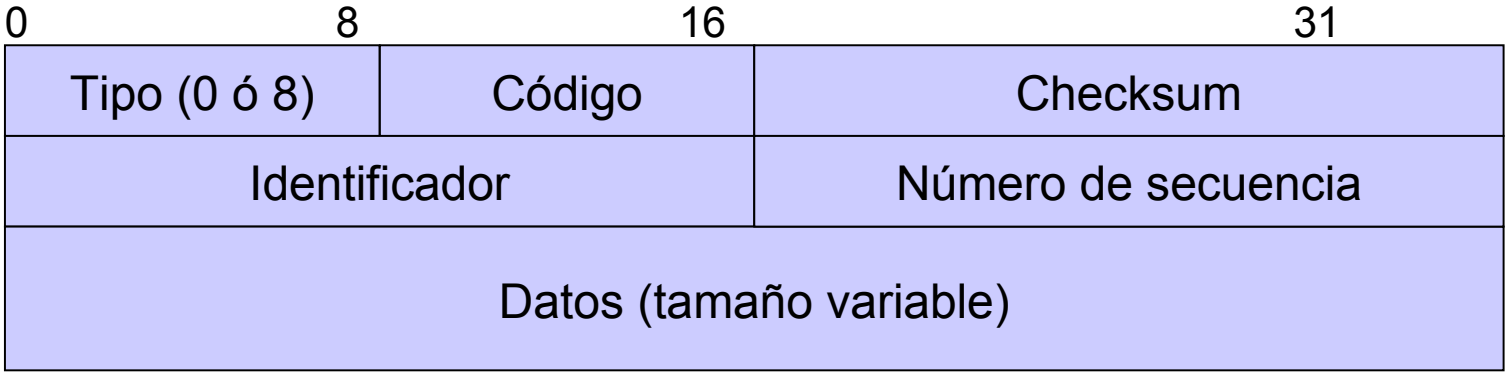
Introducción

- Formato de mensaje ICMP:
  - Tipo: identifica el tipo de mensaje ICMP (hay 15 distintos)
  - Código: utilizado en algunos códigos para especificaciones más detalladas.
  - Checksum: cubre al mensaje ICMP completo (mismo algoritmo que para el checksum de IP)



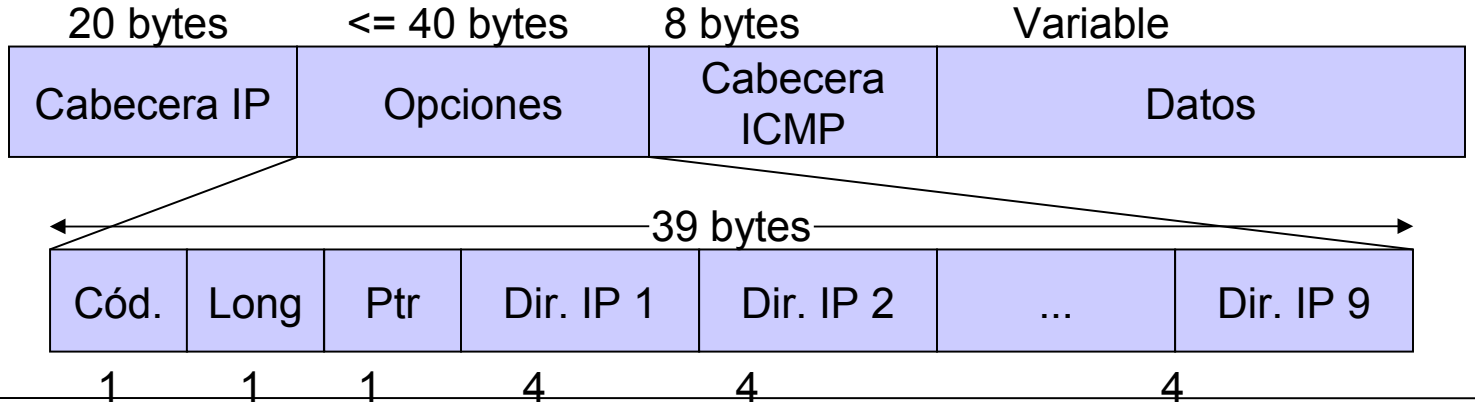
ICMP Ping

- Packet InterNet Grouper: herramienta de diagnóstico que comprueba si un nodo de la red es alcanzable.
- Cliente: Envía ICMP echo request
- Servidor: Responde con ICMP echo reply
- Formato mensajes ICMP echo request y reply:
  - Identificador: en UNIX es el identificador del proceso.
  - Número de secuencia: inicialmente 0, y se incrementa con cada echo request.
- Existen variedad de implementaciones (presentación de resultados, opciones del programa...).



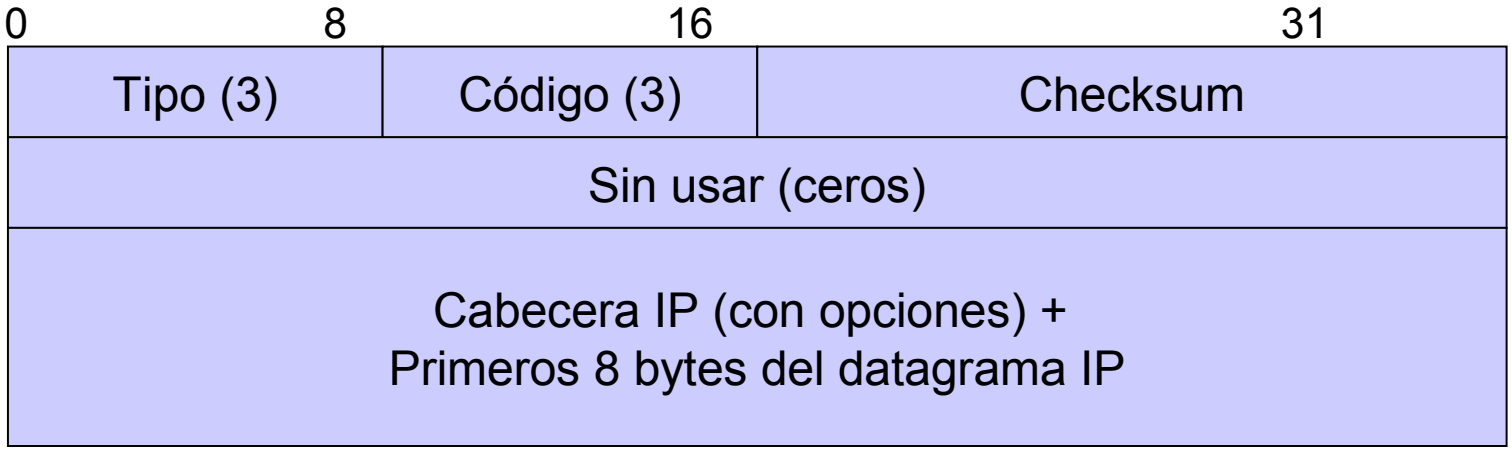
ICMP Ping: Opciones

- Opción IP de registro de ruta: se van registrando en la cabecera IP los routers por los que pasa el mensaje.
  - Los routers deben implementar esta opción (almacenan IP de salida)
  - Problema: espacio limitado en cabecera IP (40 bytes → máximo 9 direcciones IP)
- Opción IP de timestamp: registra el instante de tiempo (milisegundos desde medianoche) por el que pasa en cada router.
  - Modos de operación: registra únicamente timestamps, registra direcciones IP y timestamps (máximo 4), el emisor inicializa la lista con 4 direcciones IP, y si el router es una de ellas registra su timestamp.

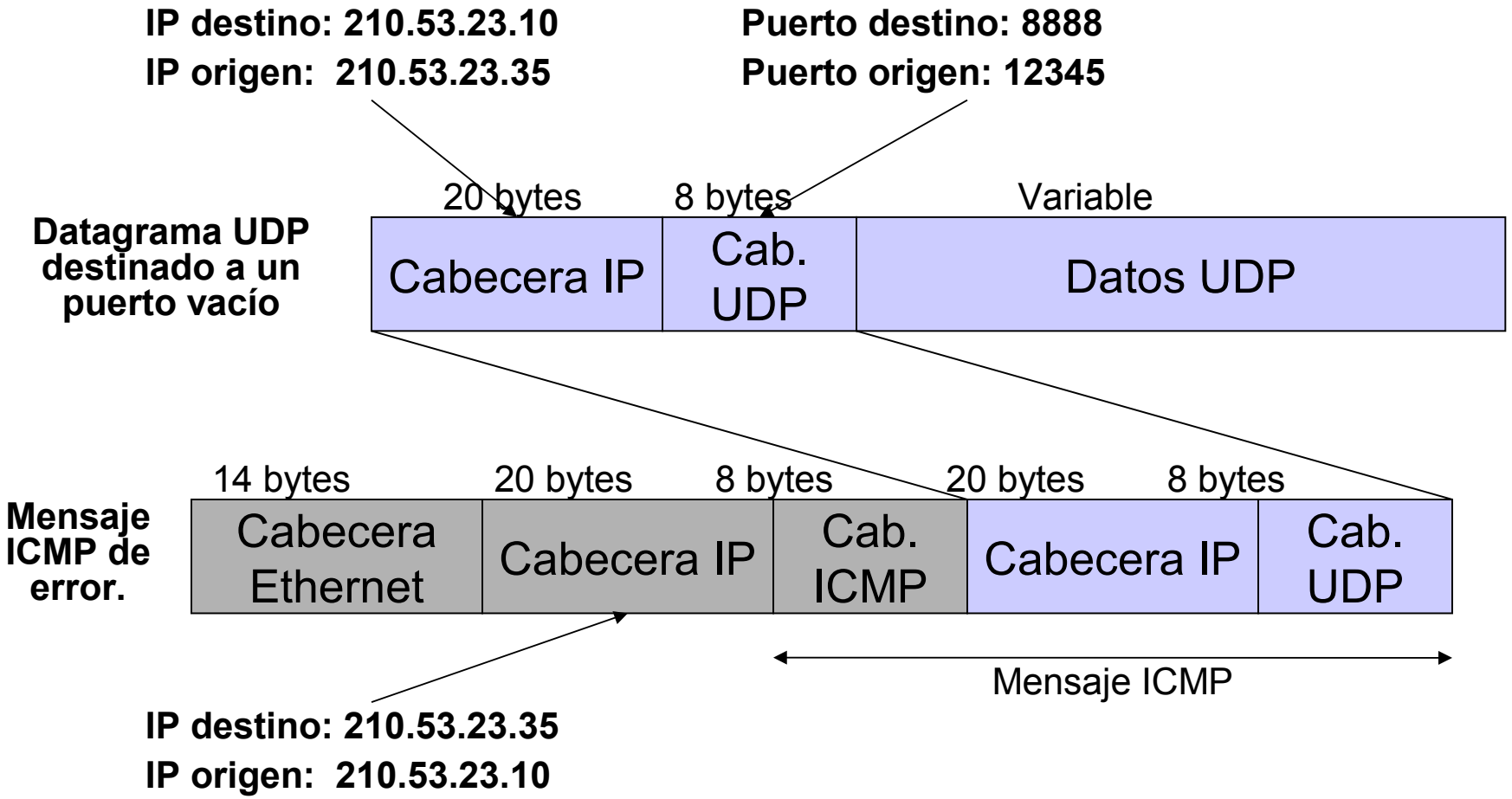


ICMP: Puerto inalcanzable

- Mensaje de error utilizado por UDP, cuando el destino no dispone de un proceso en el puerto de destino:
  - Se incluye la cabecera del mensaje que provocó el error.
    - IP de destino y origen
    - Protocolo incluido en el campo de datos
  - Y los primeros 8 bytes del datagrama IP = Cabecera UDP (incluye puerto destino y origen)

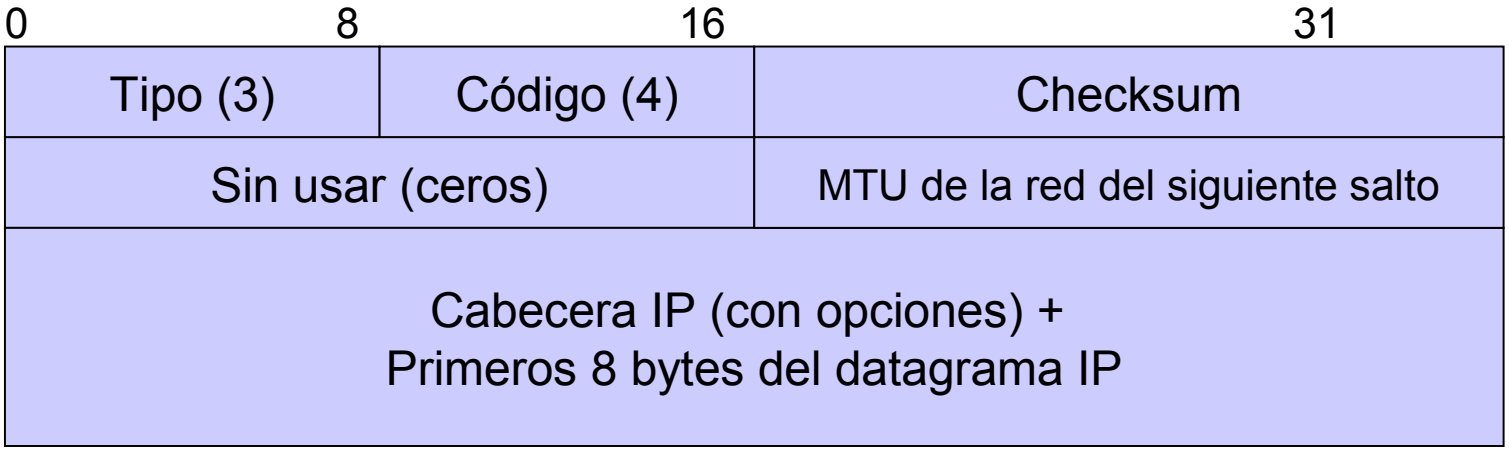


ICMP: Puerto inalcanzable



ICMP: Fragmentación requerida

- Mensaje de error utilizado por un router cuando tiene que fragmentar un datagrama IP pero tiene el flag DF activado.
  - Incluye el MTU de la red que provocó el error y la cabecera del mensaje que provocó el error.

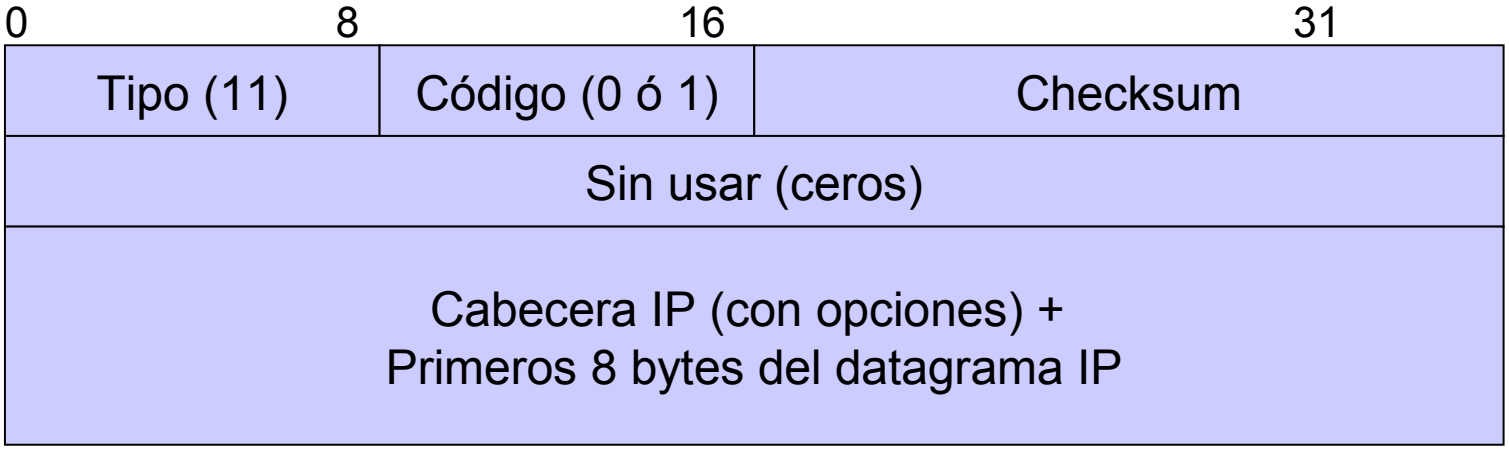


ICMP: Fragmentación requerida

- Este mensaje de error es utilizado en un mecanismo denominado **Path MTU discovery** que permite averiguar el MTU mínimo durante una comunicación y reducir la fragmentación IP (sólo se hace en origen).
  - Path MTU: MTU mínimo en cualquier red en el camino entre dos hosts.
- Funcionamiento del Path MTU discovery:
  - Se habilita el bit DF (Don't Fragment) en los datagramas enviados.
  - Si algún router en el camino necesita fragmentar → Generará el mensaje ICMP Fragmentación requerida
  - Si se recibe un mensaje ICMP Fragmentación requerida con el nuevo MTU:
    - Si eran datos TCP → TCP debe reducir el tamaño del segmento (en base al nuevo MTU) y retransmitir.
    - Sino (p.e. UDP) → IP fragmenta los datagrama en base al nuevo MTU.
  - Como las rutas cambian dinámicamente → Se puede probar un MTU mayor pasado un cierto intervalo (RFC 1191 recomienda 10 minutos).

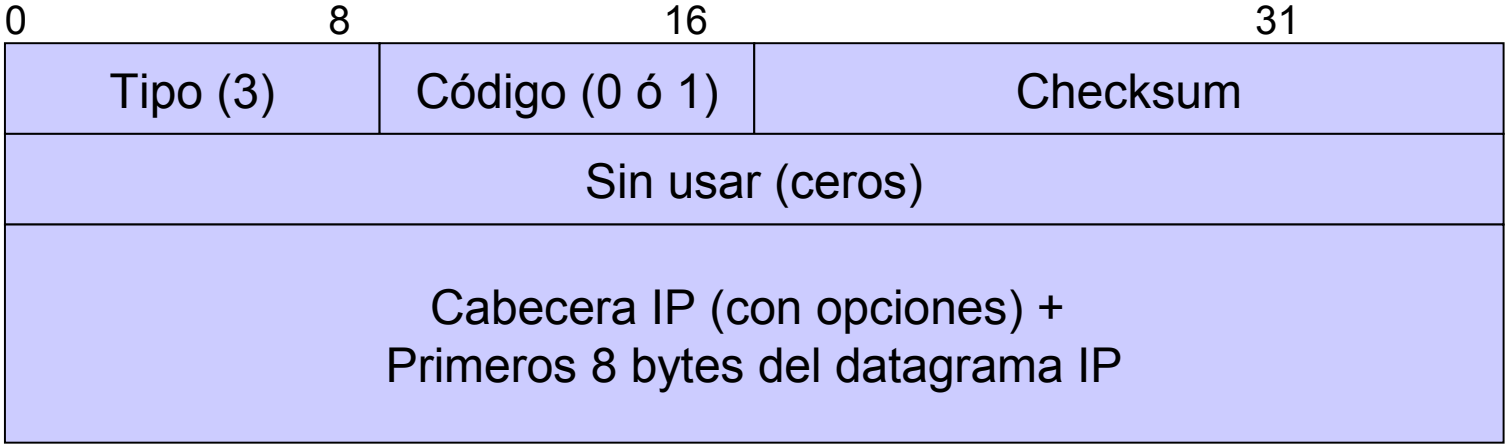
ICMP: Tiempo excedido

- Código 0: TTL = 0 durante el tránsito
- Código 1: tiempo máximo de reensamblado excedido
  - Se produce en la fragmentación IP al perderse uno de los fragmentos



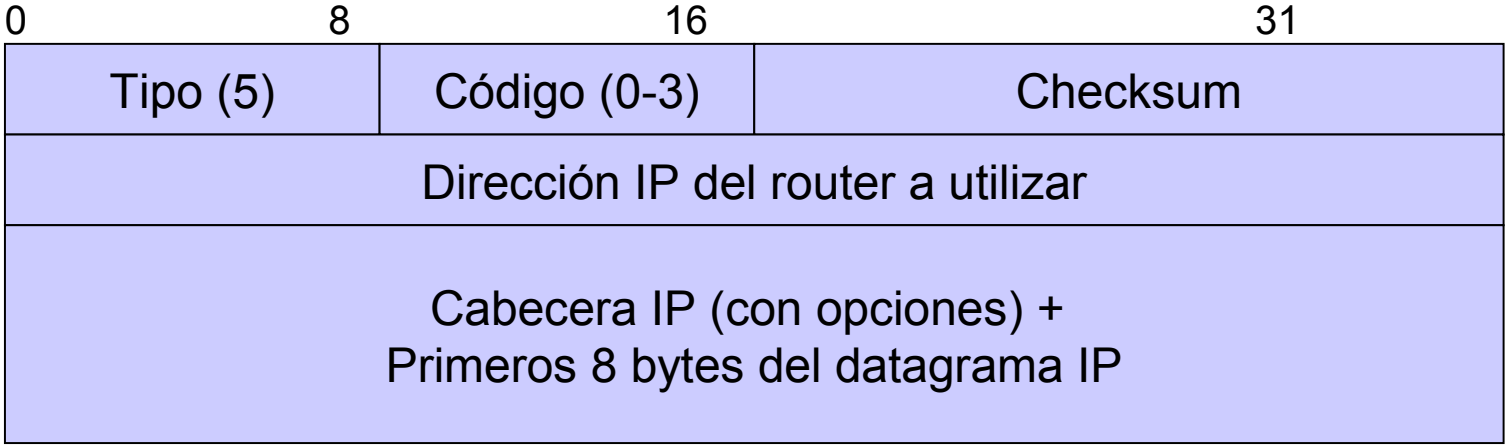
ICMP máquina o red inalcanzable

- Lo envía un router cuando no puede entregar o reenviar un datagrama IP.
- Máquina inalcanzable (código 1): si el router conoce la red, pero el host no está alcanzable en ese momento (p.e. está apagado).
- Red inalcanzable (código 0): si el router no conoce la red → No es una de sus entradas y no tiene entrada por defecto.
- Máquina o red administrativamente inalcanzables (código 10 y 9): existe un mecanismo de filtrado de paquetes (p.e. un firewall) que impide alcanzar la máquina o la red.



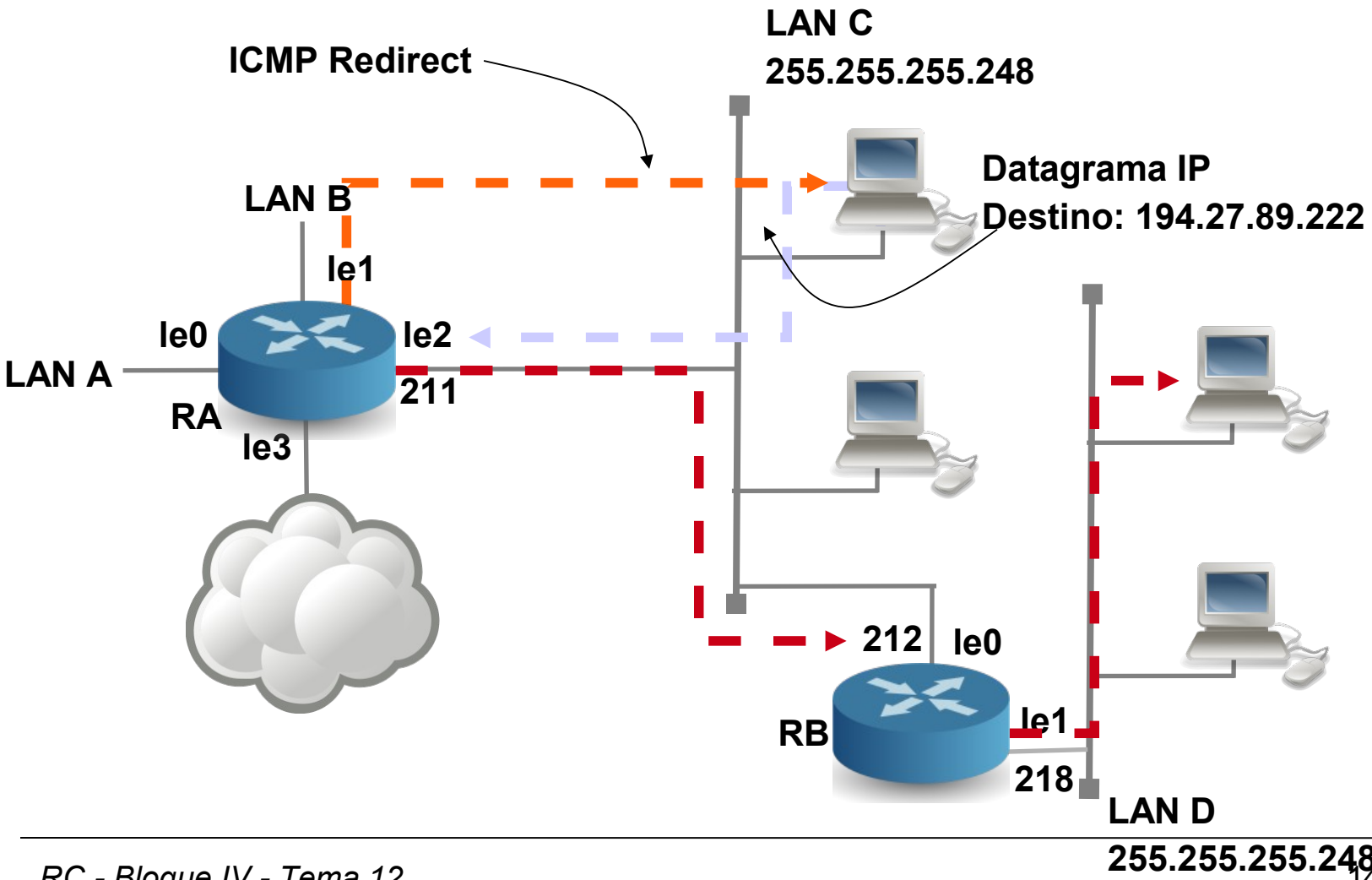
ICMP Redirect

- Mensaje de error ICMP que envía un router al remitente de un datagrama IP que debería haber sido enviado a otro router.
  - Sólo generados por routers, no por máquinas.
  - Sólo son utilizados por máquinas, no por routers.
- Esto sólo puede ocurrir cuando haya varias posibilidades de router intermedio para la máquina que hace el envío.
- Flags de la tabla de enrutamiento del redirect:
  - D: Ruta creada por un ICMP redirect
  - M: Ruta modificada por un ICMP redirect
- Se genera un mensaje ICMP redirect cuando:
  - La interfaz de salida = interfaz de entrada



ICMP Redirect

- Red 194.27.89.0 (ping desde 210 a 222)

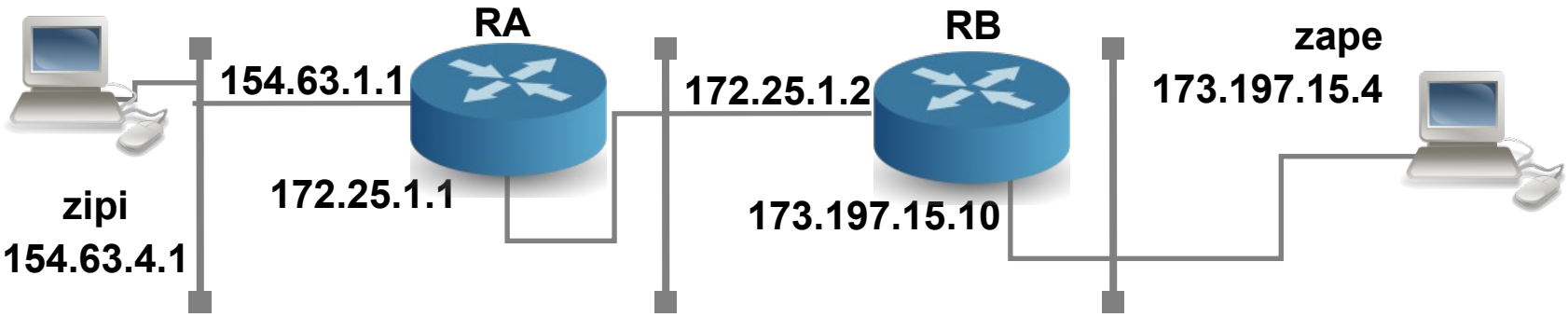


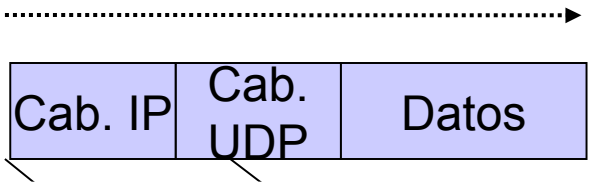
Traceroute

- Problemas del ping con registro de ruta:
  - Falta de espacio en la cabecera IP
    - Registro de ruta: máximo 9 routers
    - Timestamp: máximo 4 routers (o 9 timestamps sin direcciones IP)
  - No todos los routers soportan la opción de registro de ruta
  - No hay control sobre los relojes de los routers
- Solución: **traceroute**
  - Herramienta de diagnóstico que permite ver la ruta que sigue un datagrama, además de permitir encaminamiento en origen.

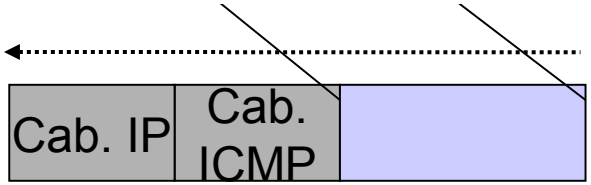
- Se basa en: datagramas UDP, el campo TTL de la cabecera IP y los mensajes de error ICMP Puerto inalcanzable y Tiempo excedido
  - Sólo requiere que el protocolo UDP esté operativo en el destinatario.
  - Cuando un router al decrementar el campo TTL obtiene 0 → Genera un mensaje de error ICMP Tiempo excedido
  - Cuando UDP recibe un datagrama para un puerto vacío → Genera un mensaje de error ICMP Puerto inalcanzable

Traceroute: Funcionamiento





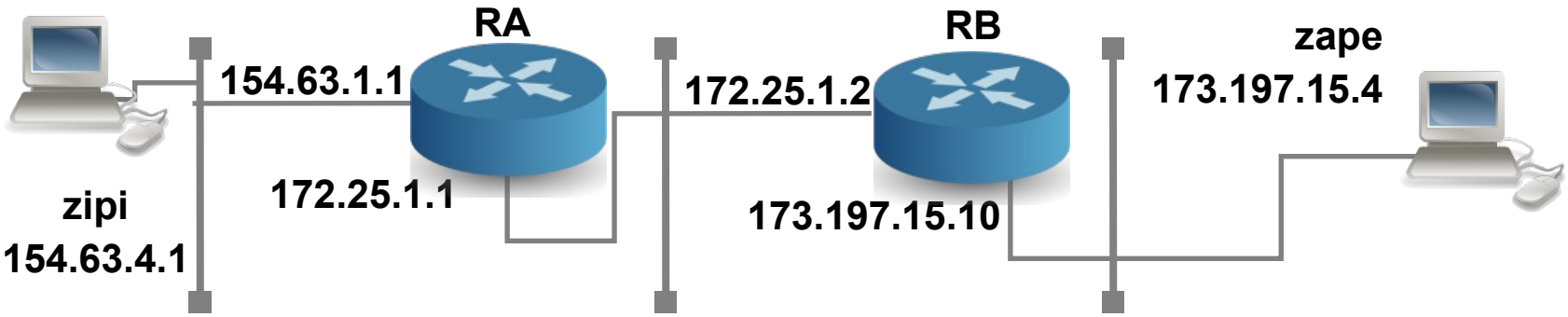
IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL = 1

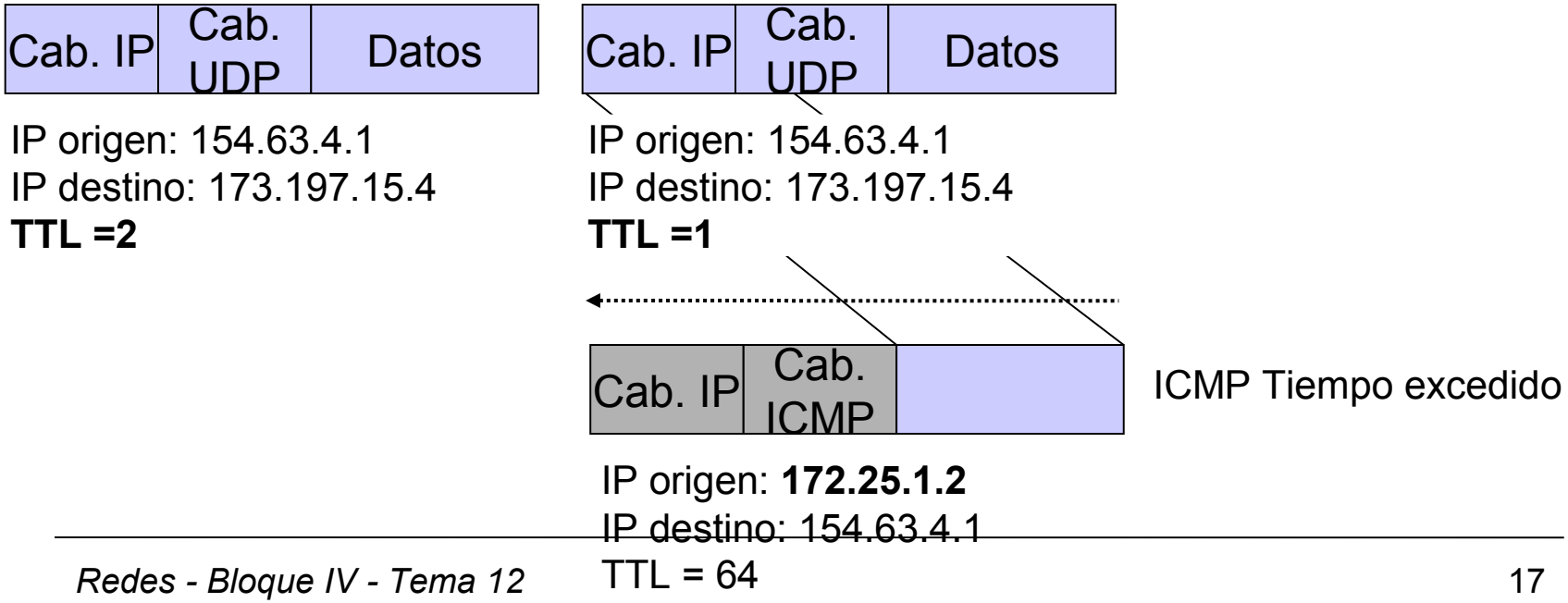


ICMP Tiempo excedido

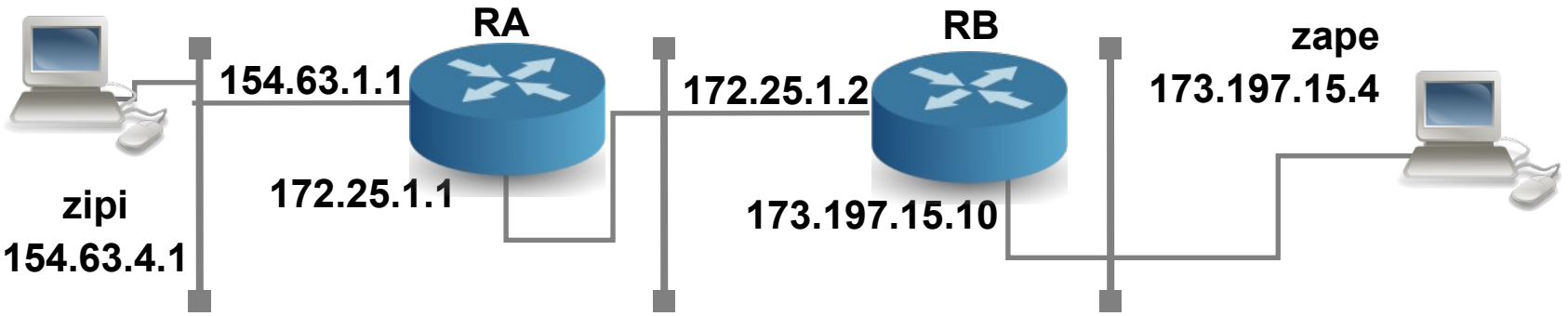
IP origen: **154.63.1.1**
IP destino: 154.63.4.1
TTL = 64

Traceroute: Funcionamiento





Traceroute: Funcionamiento



Cab. IP	Cab. UDP	Datos

IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL =3

Cab. IP	Cab. UDP	Datos

IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL =2

Cab. IP	Cab. UDP	Datos

Puerto destino: 33348
IP origen: 154.63.4.1
IP destino: 173.197.15.4
TTL =1

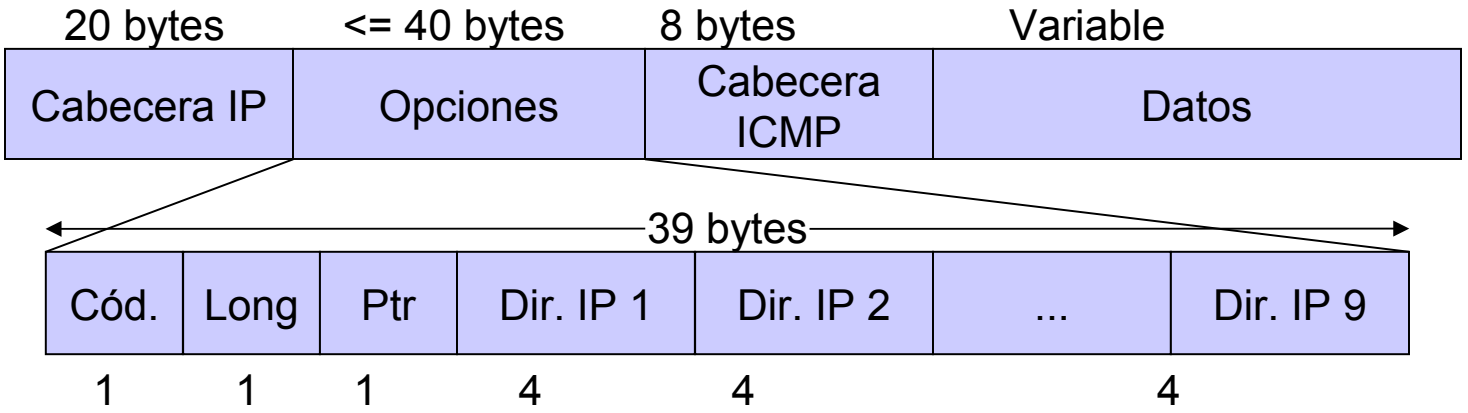
ICMP Puerto inalcanzable

Cab. IP	Cab. ICMP	

IP origen: **173.197.15.4**
IP destino: 154.63.4.1
TTL = 64

Traceroute: encaminamiento en origen

- Opción IP que permite especificar la ruta desde el origen:
  - Encaminamiento en origen estricto: lista de routers con el camino exacto desde origen al destino. Si falta algún router → ICMP "source route failed".
  - Encaminamiento en origen difuso: lista de routers por los que el paquete debe pasar, pero también puede pasar por otros routers.



Resumen

- Principales comandos de red:
  - **ifconfig**: ver configuración de red.
  - **netstat**: ver puertos ocupados y más cosas.
  - **nslookup** y **dig**: enviar peticiones DNS.
  - **route**: ver y modificar la tabla de enrutamiento.
  - **ping**
  - **traceroute**
    - Versión gráfica: http://www.yougetsignal.com/tools/visual-tracert/